RED TEAM

PENETRATION TESTING

FIND THE GAPS. BEFORE OTHERS DO.

Know what an attacker would find before they come looking.

Penetration testing and continuous vulnerability management, built for K-12 school districts and the people who keep them running.

FIND THE GAPS. BEFORE OTHERS DO.

Blue Ridge IT Solutions

DEDICATED TO K12 AND THOSE WHO SERVE IT

blueridge-us.com

423.292.1922

info@blueridge-us.com

THE PROBLEM

School districts are now a primary target.

Districts hold exactly what attackers want — student and family records, staff payroll and banking detail, and networks that must stay open to thousands of devices. They are also expected to defend that environment with a fraction of the staff and budget of the private sector.

24/7

Your network is reachable around the clock — attackers do not work school hours.

1 click

A single phishing click can hand an outsider the same view your staff have.

Days

Instruction lost when an incident takes systems offline district-wide.

The question is no longer whether your district has exposures. It is whether you find them first.

Automated tools produce long lists. What a district actually needs is a short, ranked, verified list of what a real attacker could use — and a plan to close it.

Ransomware stops school

An incident does not just cost money — it cancels instruction, exposes families, and becomes a public event the board will ask about for years.

Student data carries obligations

Districts are custodians of protected student records. Actively testing and remediating your environment is part of meeting that duty.

Insurers and grants now ask

Cyber-liability renewals and funding applications increasingly require evidence of vulnerability assessment and penetration testing.

Small teams, large surface

One or two people often cover every building and system. You do not need more alerts — you need the few things that matter most.

THE SERVICE

Offensive testing, delivered as a service.

We assess your district the way an attacker would: discover everything on the network, find the weaknesses, safely prove which ones are genuinely exploitable, and hand your team a prioritized plan to fix them. Run it once as a point-in-time assessment, or continuously as an ongoing program.

HOW AN ENGAGEMENT RUNS

1. **Scope** — Written authorization, agreed targets, and any systems explicitly excluded.
2. **Discover** — Full inventory of live hosts, services and platforms across the environment.
3. **Assess** — Deep testing, internal and external, with and without credentials.
4. **Validate** — Safe confirmation of what is genuinely exploitable.
5. **Report** — Board-ready summary plus full technical detail.
6. **Remediate** — We track fixes to closure and re-test to prove it is gone.

DISCOVERY & VISIBILITY

Complete asset discovery

Every device on the network found, fingerprinted and inventoried — including the ones nobody remembers putting there.

Network mapping

A visual map of your environment by subnet, with each host scored by real risk so you can see where exposure concentrates.

Service & platform identification

Open ports, running services, versions and operating systems catalogued for every host.

Perimeter & internal testing

We assess both what the internet can see and what an attacker already inside would see.

ENGAGEMENT MODELS

Point-in-time

A single comprehensive assessment with a full report — ideal for insurance renewals, grant applications, or establishing a baseline.

Recurring

Scheduled reassessments through the school year, so remediation is verified and new exposure is caught as the environment changes.

Continuous

Always-on assessment with ongoing tracking and reporting — the strongest posture and the clearest evidence of due diligence.

CAPABILITIES

What we test, and how we prioritize it.

VULNERABILITY ASSESSMENT

Authenticated & unauthenticated

Testing with and without credentials — what is exposed publicly, and what a compromised account could reach.

Web application testing

District websites, portals and internally hosted applications assessed for common and critical weaknesses.

Configuration & hardening review

Weak settings, legacy protocols, default credentials and unnecessary exposure identified.

Credential strength auditing

Password and authentication weaknesses surfaced before someone else finds them.

THREAT INTELLIGENCE & PRIORITIZATION

Live threat intelligence

Every finding enriched against global vulnerability intelligence, refreshed continuously — not a static checklist.

Actively-exploited flagging

Vulnerabilities known to be under active attack in the wild are called out and pushed to the top of your list.

Ransomware association

Weaknesses tied to known ransomware campaigns are highlighted explicitly.

Severity & risk scoring

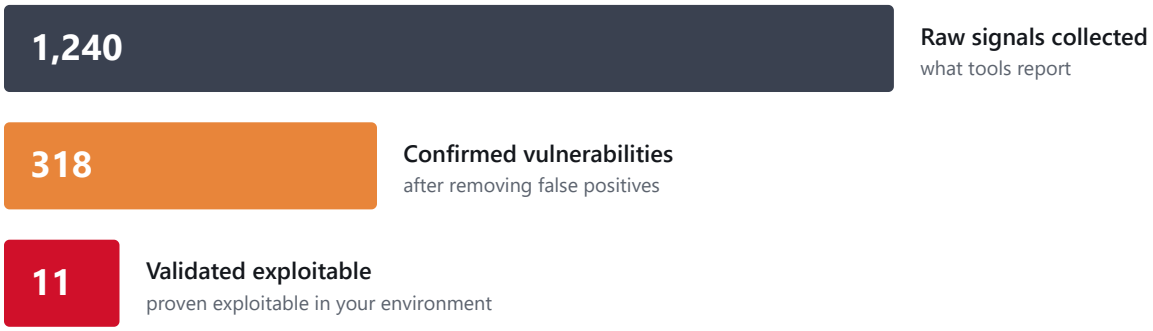
Industry-standard severity plus a district-level risk score that tracks your posture over time.

Safety first, always. Every engagement begins with written authorization and a defined scope. Excluded systems are honored, testing is scheduled around instructional time, destructive and denial-of-service techniques are never used, and every action taken is logged in a full audit trail you can review.

THE DIFFERENCE

Proof, not theory.

Anyone can hand you a scan. The hard part — and the part that protects your district — is proving which of those findings an attacker could actually use. We safely validate exploitability and strip out the noise, so your team works a list it can trust.



Illustrative of a typical district assessment. Actual counts vary by environment size.

Most tools tell you what might be wrong. We tell you what is actually exploitable.

That is the difference between a 400-item report nobody can action and a short list your team can close this month.

False positives removed

You get a remediation list your team can trust, not hundreds of items that turn out to be noise.

Non-disruptive by design

Safe checks by default. Destructive and denial-of-service techniques are excluded from every engagement.

Evidence captured

Each validated finding is documented with the supporting evidence your auditors, board or insurer may ask for.

Tracked to closure

Status moves from open to confirmed to remediated, so progress is measurable between assessments.

WHAT YOU RECEIVE

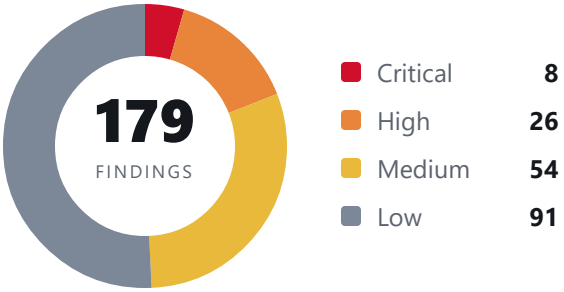
A report written for two audiences.

One document your superintendent and board can read, and the technical depth your IT staff need to actually fix things — plus a posture score you can track from assessment to assessment.

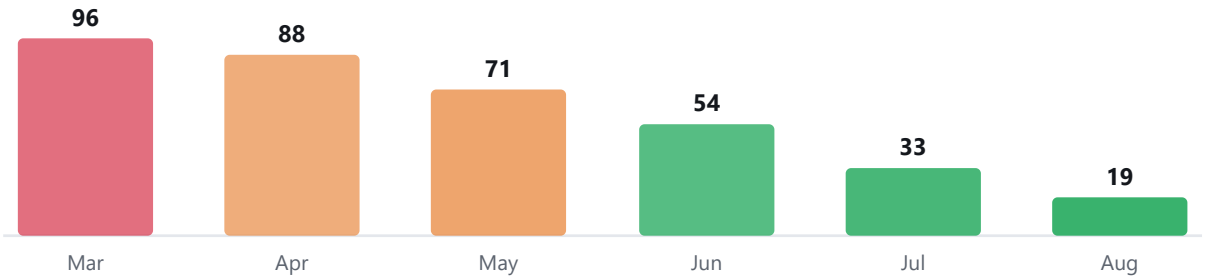
DISTRICT RISK POSTURE

Weighted by severity, exploitability and active-exploitation status.

FINDINGS BY SEVERITY



EXPOSURE TREND — REMEDIATION PROGRESS



Open high-and-critical findings, measured each month. Evidence of due diligence over time — the chart insurers and boards want to see.

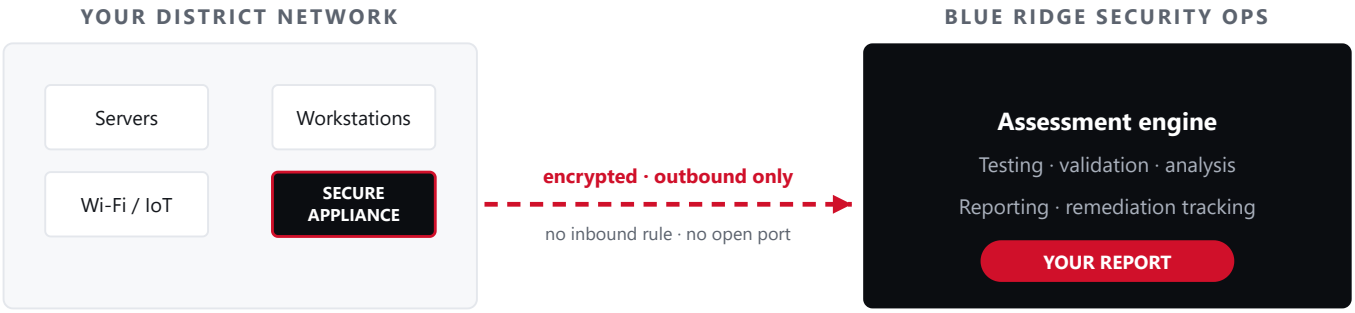
Sample visuals shown for illustration.

- ✓ **Executive summary** — plain language for the superintendent, board and cabinet.
- ✓ **Risk posture score** — one number, tracked over time.
- ✓ **Prioritized roadmap** — what to fix first, second and third.
- ✓ **Full technical detail** — every finding with affected hosts and evidence.
- ✓ **Remediation guidance** — specific steps written for your IT staff.
- ✓ **Branded PDF** — suitable for insurers, auditors and board packets.

DEPLOYMENT

Nothing to buy. Nothing to open on your firewall.

Internal testing runs from a lightweight secure appliance on infrastructure you already have. It makes an encrypted outbound connection to us — there is no inbound access, no port to open, and no hardware to purchase.



Simple to deploy

Your team imports one file and powers it on. It connects automatically and is ready to assess — typically in minutes, with no on-site visit required.

Outbound only

The appliance reaches out to us over an encrypted tunnel. Nothing is exposed to the internet and no inbound firewall rule is ever required.

Inside and outside

We assess your internet-facing perimeter and, through the appliance, your internal network — the view an attacker gets after one phishing click.

Recurring by schedule

Assessments run on a schedule so your posture is measured continuously, not once a year.

0
Inbound firewall rules required.

0
Hardware purchases required.

Minutes
From power-on to first assessment.

RED TEAM
PENETRATION TESTING
FIND THE GAPS. BEFORE OTHERS DO.

Let's find the gaps in your district — first.

We will walk your team through a sample assessment, scope an engagement around your calendar, and show you exactly what the deliverable looks like before you commit to anything.

START THE CONVERSATION

423.292.1922 · info@blueridge-us.com

blueridge-us.com

BLUE RIDGE
IT SOLUTIONS
SMART SOLUTIONS. STRONGER BUSINESS.

DEDICATED TO K12 AND THOSE WHO SERVE IT